ABSTRACT:

The invention relates to a method of copy-protection of information stored on an information carrying medium. The method allows a reading device (e.g. a DVD drive) and an application device (e.g. an MPEG decoder) to exchange copy-protection information regarding the information carrying medium (e.g. an optical record carrier like a CD or DVD) and the content on that medium. The method is cryptographically secure, taking into account the situation where reading device and application device are connected to an open bus in a personal computer. In view of the high-volume nature of the drive, the method can be implemented cheaply. The inventive method is robust against a so-called man-in-the-middle attack.

The invention relates also to a method of exchanging copy-protection information, to a copy-protection system and to devices for carrying out these methods, in particular a reading device, an application device and a device for playback and/or recording of information.